CLAIMS

1. A system for user authentication using infrared communication of a mobile terminal, comprising:

a mobile terminal for generating electronic signature data for a user who requests a particular service in the form of an infrared signal with a view to performing a step of user authentication;

automated information providing means for verifying the electronic signature data provided by the mobile terminal and for allowing the requested service depending on the verification result; and

certificate providing means for registering a certificate in response to a request for issuance of the certificate by the mobile terminal and for transmitting the certificate to the automated information providing means through a communication network with a view to verifying the validity of user authentication.

2. The system set forth in claim 1, wherein the mobile terminal possesses applications including a security library for providing information required for processing of security service with being linked to a security service program, a certificate storing unit for storing the certificate provided by the certificate providing means, a certificate issuance processing module for processing tasks required for letting the certificate providing means issue a certificate by generating a pair of a private key and a public key, a security service module for providing security service for issuance of the certificate and processing of the electronic signature data, a certificate management module for managing the issued certificate, and an electronic signature service module for performing an electronic signing and data

encryption and decryption using the issued certificate.

3. The system set forth in claim 2, wherein the mobile terminal includes an infrared communication processing unit for transmitting/receiving an infrared signal for user authentication by transmitting the electronic signature data in the form of an infrared signal.

4. The system set forth in claim 1, wherein the automated information providing means comprises a keypad for receiving user input for requesting the particular service, an infrared communication unit for transmitting/receiving an infrared signal for user authentication by receiving the electronic signature data from the mobile terminal, a control module for controlling the progress of the particular service by verifying the validity of the electronic signature data from the mobile terminal using the certificate provided by the certificate providing means, a security library for providing information required for verification of the electronic signature data in conjunction with a validation control function of the control module, a network interface adaptor for exchanging data for user authentication by connecting to the certificate providing means through a communication network, and an information providing module for providing the requested service under the control of the control module.

5. The system set forth in claim 4, wherein the control module belonging to the automated information providing means receives the certificate and a certificate revocation list from the certificate providing means, verifies the validity of the certificate based on the certificate revocation list, and performs the verification of the electronic signature data and authentication of the user using the certificate.

6. The system set forth in claim 1 or claim 5, wherein the mobile terminal and the automated information providing means exchange the electronic signature data by way of OBEX

(Object Exchange Services) included in a protocol stack for the infrared communication.

7. A method for user authentication using infrared communication of a mobile terminal, comprising:

a first step at which a request for a particular service is sent from a mobile terminal to automated information providing means;

a second step, responsive to a request for electronic signature data from the automated information providing means, of transmitting electronic signature data created by the mobile terminal to the automated information providing means by way of infrared communication;

a third step, conducted by the automated information providing means, of obtaining a certificate registered by the mobile terminal from certificate providing means through a communication network;

a fourth step, conducted by the automated information providing means, of performing user authentication by verifying the validity of the certificate and the electronic signature data; and

a fifth step of allowing the requested service if the user authentication is successful.

8. The method set forth in claim 7, wherein the second step comprises:

a first substep at which an infrared receiving mode is started by the automated information providing means, and an electronic signing is performed by the mobile terminal;

a second substep of initializing communication between the automated information providing means and the mobile terminal;

a third substep, conducted by the automated information providing means, of requesting the electronic signature; and

a fourth substep, conducted by the mobile terminal, of

transmitting the electronic signature data in the form of an infrared signal.

9. The method set forth in claim 7, wherein the third step comprises the steps of:

c1) referring to the certificate providing means for the certificate for the user of the mobile terminal through the communication network;

c2) obtaining the certificate registered by the user of the mobile terminal; and

c3) obtaining the certificate revocation list.

10. The method set forth in claim 7 or 9, wherein the fourth step comprises the steps of:

d1) verifying the validity of the certificate based on the received certificate revocation list;

d2) verifying the electronic signature data using the validated certificate; and

d3) performing user authentication based on the user identification information included in the certificate.